UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/791,322	03/02/2004	Dmitry Andreev	END920030143	1826

7590 07/22/2008

Andrew M. Calderon
Greenblum and Bernstein P.L.C.
1950 Roland Clarke Place
Reston, VA 20191

EXAMINER	
TABOR, AMARE F	

ART UNIT	PAPER NUMBER
2139	

MAIL DATE	DELIVERY MODE
07/22/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/791,322	ANDREEV ET AL.	
	Examiner	Art Unit	
	AMARE TABOR	2139	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *22 April 2008*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1,3-10,13-19 and 21-25* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1, 3-10, 13-19 and 21-25* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This correspondence is in response to **Amendments** and **REMARKS** filed on April 22, 2008.

2. Claims 1, 3, 9, 13-15, 21 and 22 are amended; Claims 2, 11, 12 and 20 are cancelled; and Claims 23-25 are new.

3. **Claims 1, 3-10, 13-19 and 21-25** are pending.

Response to Arguments

4. Applicant's arguments with respect to the pending claims have been considered but are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 103

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1, 3-5, 8-10, 13, 14 and 22 are rejected under 35 U.S.C. 103(a) as being unpatentable over Young et al. (US 7,024,690 B1 - "Young") in view of Kaufman et al. (US 5,497,421 - "Kaufman"), and further in view of Blanco et al. (US 6,539,482 B1 - "Blanco")

As per Claim 1, Young teaches,

A method for authentication in a network, the method comprising: creating a credential string on a portal server [see **Client System 220** in FIG.2; and for example, col.4, lines 47-67], the credential string being an encrypted hash of a session ID [see FIG.3; and for example, col.5, lines 9-19]; and sending a UserID associated with the session ID and the credential string to a software application from the portal server [see **AP 210** in FIG.2 and FIG.3; and for example, col.5, lines 1-8].

Young teaches communicating hashed representation of user identifiers and passwords [see FIG.3 and abstract]; but fails to disclose maintaining the user password on the portal server and avoiding exposing the user password to network resources beyond the portal server. However, in the same field of endeavor, Kaufman discloses maintaining the user password on the portal server and avoiding exposing the user password to network resources beyond the portal server [see for example, FIGS.3-5 and abstract].

Therefore, it would have been obvious to a person having ordinary skill in the art, at the time of Applicants' invention, to combine the teachings of Young and Kaufman because both are in the fields of network authentication system. Incorporating Kaufman's teaching modifies the system of Young in order to protect the confidentiality of user's password [see abstract of **Kaufman**].

Young-Kaufman combination teaches confirmation request including the credential string [see for example, FIG.3 of **Young** and FIGS.3-5 of **Kaufman**]; but fails to disclose receiving a confirmation request from the software application to an LDAP; and sending a response from the LDAP proxy in reply to the confirmation request to validate the credential string to authenticate the UserID. Nevertheless, Blanco teaches receiving a confirmation request from the software application to an LDAP; and sending a response from the LDAP proxy in reply to the confirmation request to validate the credential string to authenticate the UserID [see for example, FIG.2 and abstract].

It would have been obvious to a person having ordinary skill in the art, at the time of Applicants' invention, to modify Young-Kaufman combination by incorporating Blanco's LDAP, so that users could access network service, which includes a directory, remotely or locally [see abstract of **Blanco**].

As per Claim 9, Young teaches,

A method for authenticating a user request for a software application, the method comprising: receiving a UserID and a credential string at an authentication proxy server, the credential string being an encrypted hash of a session ID, which is created at a portal [see **Client System 220** in FIG.2; and for

example, col.4, lines 47-67]; and sending a confirmation request from the authentication proxy to the a portal [see **AP 210** in FIG.2 and FIG.3; and for example, col.5, lines 1-8].

Young teaches communicating hashed representation of user identifiers and passwords [see for example, FIG.3 and abstract]; but fails to disclose maintaining the user password on the portal server and avoiding exposing the user password to network resources beyond the portal server. However, in the same field of endeavor, Kaufman discloses maintaining the user password on the portal server and avoiding exposing the user password to network resources beyond the portal server [see for example, FIGS.3-5 and abstract].

It would have been obvious to a person having ordinary skill in the art, at the time of Applicants' invention, to modify the system of Young by incorporating Kaufman's teaching in order to protect the confidentiality of user's password [see abstract of **Kaufman**].

Young-Kaufman combination teaches confirmation request including the credential string [see for example, FIG.3 of **Young** and FIGS.3-5 of **Kaufman**]; but fails to disclose receiving a confirmation request from the software application to an LDAP; and sending a response from the LDAP proxy in reply to the confirmation request to validate the credential string to authenticate the UserID. Nevertheless, Blanco teaches receiving a confirmation request from the software application to an LDAP; and sending a response from the LDAP proxy in reply to the confirmation request to validate the credential string to authenticate the UserID [see for example, FIG.2 and abstract].

It would have been obvious to a person having ordinary skill in the art, at the time of Applicants' invention, to modify Young-Kaufman combination by incorporating Blanco's LDAP, so that users could remotely or locally access network services [see abstract of **Blanco**].

As per Claim 22, Young-Kaufman-Blanco combination teaches,

A computer program product comprising a computer usable medium having readable program code embodied in the medium, the computer program product including at least one program code to:

create a credential string on a portal server, the credential string being an encrypted hash of a session ID [see **Client System 220** in FIG.2; and for example, col.4, lines 47-67 of **Young**];

send a UserID associated with the session ID and the credential string to a software application from the portal server [see **AP 210** in FIG.2 and FIG.3; and for example, col.5, lines 1-8 of **Young**], while maintaining the user password on the portal server and avoiding exposing the user password to network resources beyond the portal server [see for example, FIGS.3-5 and abstract of **Kaufman**]:

the confirmation request including the credential string [see for example, FIG.3 of **Young** and FIGS.3-5 of **Kaufman**]; receive a confirmation request from the software application to an LDAP proxy while maintaining the user password on the portal server such that the user password is not required to authenticate the User ID; and send a response from the LDAP proxy in reply to the confirmation request to validate the credential string to authenticate the UserID [see for example, FIG.2 and abstract of **Blanco**].

As per Claim 3, Young-Kaufman-Blanco combination teaches,

wherein the encrypted hash of the session ID is a derivate of the session ID [see for example, FIG.3 of **Young** and abstract of **Kaufman**].

As per Claim 4, Young-Kaufman-Blanco combination teaches,

performing a lightweight directory access protocol (LDAP) lookup using the UserID; and if the LDAP lookup confirms the UserID and the response validates the credential string [see for example, FIG.2 of **Blanco**], returning a successful authentication reply to the software application for establishing a session associated with the session ID [see for example, **Grant Access 112** in FIG.3 of **Blanco**, otherwise sending an unsuccessful authentication reply to the software application [see for example, **Deny Access 106** in FIG.3 of **Blanco**].

As per Claim 5, Young-Kaufman-Blanco combination teaches,

wherein the sending of a UserID and the credential string avoids at least one of sending a user's password outside of a portal server and storing the password in persistent memory [see for example, FIGS.3-5 and abstract of **Kaufman**].

As per Claim 8, Young-Kaufman-Blanco combination teaches,

wherein the receiving step and sending a response step is performed by an authentication proxy [see for example, **AP 210** of **Young**; **LOGIN AGENT (LA) NODE 26** of **Kaufman**; and **LDAP Client** of **Blanco**].

As per Claim 10, Young-Kaufman-Blanco combination teaches,

providing a confirmation to the software application if the response is affirmative and the UserID is authenticated by the LDAP lookup [see for example, FIGS.2 and 3 of **Blanco**].

As per Claim 13, Young-Kaufman-Blanco combination teaches,

validating the confirmation request by assuring that the credential string has been received only once for confirmation at the portal, otherwise, if presented more than once, performing at least one of initiating a security breach procedure and notifying a software application proxy [see for example, FIGS.2 and 3 – *where **Blanco** discloses credential single receiving*].

As per Claim 14, Young-Kaufman-Blanco combination teaches,

receiving the UserID and the user password during a logon to the portal, wherein the UserID is validated in the validating step and the user password is maintained at the portal and used to process the confirmation request [see for example, FIGS.3-5 and abstract of **Kaufman**].

Claims 6, 7, 15, 19 and 23-25 are rejected under 35 U.S.C. 103(a) as being unpatentable over "Young" in view of "Kaufman", and further in view of Wenisch et al. (US 7,100,054 B2 - "Wenisch")

As per Claim 15, Young teaches,

A system for authenticating a session stored on a computer readable storage medium, comprising computer readable program code, comprising: an authentication proxy which receives requests to authenticate a UserID and a credential string [see **LOGIN AGENT (LA) NODE** in FIG.2 of **Kaufman**], the credential string being an encrypted hash of a session ID and created on a portal [see **Client System 220** in FIG.2; and for example, col.4, lines 47-67 of **Young**].

Young teaches a credential string validation component which receives requests to validate the credential string [see FIG.3]; but fails to disclose maintaining a user password on the portal such that the user password is not required to validate the credential string, and avoiding exposing the user password to network resources beyond the portal. However, Kaufman teaches maintaining a user password on the portal such that the user password is not required to validate the credential string, and avoiding exposing the user password to network resources beyond the portal [see FIGS.3-5 and abstract of **Kaufman**].

It would have been obvious to a person having ordinary skill in the art, at the time of Applicants' invention, to modify the system of Young by incorporating Kaufman's teaching in order to protect the confidentiality of user's password [see abstract of **Kaufman**].

Young-Kaufman combination fails to teach wherein the credential string validation component checks whether the credential string has been previously received for validation within a predetermined time period; however, in the same field of endeavor, Wenisch teaches wherein the credential string validation component checks whether the credential string has been previously received for validation within a predetermined time period [see for example, FIG.2; and for example, col.4, lines 25-35].

Therefore, it would have been obvious to a person having ordinary skill in the art, at the time of Applicants' invention, to modify Young-Kaufman combination by incorporating the teachings of Wenisch in order to protect the network from repetitive attack.

As per Claims 6 and 7, Young-Kaufman-Wenisch combination teaches,

sending the UserID associated with the session ID and the credential string to a software application proxy [see FIGS.3 and 3-5 of **Young** and **Kaufman** respectively. See also FIG.2 of **Blanco**]; checking whether the session ID and the credential string have been previously received within a predetermined time period; and if affirmative, initiating a security breach procedure; and wherein the security breach procedure causes the termination of any session associated with the UserID [see FIG.2; and for example, col.4, lines 25-35 of **Wenisch**].

As per Claims 19 and 23, Young-Kaufman-Wenisch combination teaches,

a software application proxy which receives the UserID and the credential string and detects whether the UserID and the credential string have been previously received within a predetermined time period; and wherein the UserID and the credential string are sent to a software application when the predetermined time period has elapsed [see FIG.2; and for example, col.4, lines 25-35 of **Wenisch**].

As per Claims 24 and 25, Young-Kaufman-Wenisch combination teaches,

wherein a network security breach is initiated when a second request to validate the credential string occurs within the predetermined time period of a first request to validate the credential string [see FIG.2; and for example, col.4, lines 25-35 of **Wenisch**]; and wherein the portal is configured to accept a logon by a user and create the credential string from an associated session ID [see for example, FIG.3 of **Young** and abstract of **Kaufman**].

Claims 16-18 and 21 are rejected under 35 U.S.C. 103(a) as being unpatentable over "Young-Kaufman-Wenisch" combination, and further in view of "Blanco"

As per Claims 16-18, Young-Kaufman-Wenisch combination teaches,

wherein the authentication proxy receives the UserID and credential string from a software application [see FIGS.3 and 3-5 of **Young** and **Kaufman** respectively].

Blanco discloses wherein the authentication proxy performs lightweight directory access protocol (LDAP) lookups using the UserID and sends the credential string to the credential string validation component and receives a validation reply [see for example, FIG.2]; wherein the authentication proxy sends an affirmative authentication reply to a software application when both the LDAP lookup is successful and the validation reply indicates a valid credential string [see for example, FIG.3].

As per Claim 21, Young-Kaufman-Wenisch-Blanco combination teaches,

a lightweight directory access protocol (LDAP) directory for authenticating the UserIDs and which is accessible by the authentication proxy [see for example, FIGS.2 and 3 of **Blanco**]; and a software application proxy for intercepting the UserID and the credential string sent by the portal for monitoring duplicate occurrences of the UserID and the credential string [see FIGS.3 and 3-5 of **Young** and **Kaufman** respectively. See also FIG.2 of **Blanco**].

Conclusion

6. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to AMARE TABOR whose telephone number is (571)270-3155. The examiner can normally be reached on Mon-Fri 8:00a.m. to 5:00p.m., EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kristine Kincaid can be reached on (571) 272-4063. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Amare Tabor
(AU 2139)

/Kristine Kincaid/
Supervisory Patent Examiner, Art Unit 2139